MEDIENBRIEFING SECURITY

Liebe Medienschaffende,

die DIGITAL X bringt in Köln eine Fülle von Themen, Debatten, Impulsen und Begegnungen zusammen. Und weil man auch als schnellste Redaktion nicht überall gleichzeitig sein kann, haben wir für Sie das Wichtigste des Tages gebündelt. In diesem Informationspaket finden Sie zentrale Aussagen, relevante Themen und ausgewählte Eindrücke des Tages kompakt zusammengefasst – als journalistischen Service für Ihre Berichterstattung und als Ausgangspunkt für weitere Recherchen. Wir wünschen eine informative Lektüre – und freuen uns, wenn wir Sie bei Fragen, Interviewwünschen oder der Suche nach weiterführendem Material unterstützen können.

Ihr Presseteam der Telekom

THEMENBEREICH SECURITY

01 I Das Wichtigste auf einen Blick

Cyberabwehr – die 24/7 Frage für den Mittelstand

23.000 DDoS-Angriffe hat die Telekom allein in dieser Woche in ihrem Netz registriert und Kunden gewarnt. Auf der Digital X warnen Sicherheitsexperten vor einem steigenden Angriffstempo und einer Bedrohung, die längst nicht mehr nur die IT-Abteilung betrifft. Für Unternehmen rückt damit eine praktische Frage in den Mittelpunkt: Wer reagiert, wenn nachts um drei tatsächlich etwas passiert?

Köln. Künstliche Intelligenz beschleunigt Cyberangriffe, geopolitische Konflikte verschärfen die Bedrohungslage und Unternehmen müssen ihre Verteidigung zunehmend rund um die Uhr organisieren. Telekom-Sicherheitschef Thomas Tschersich verwies auf der Digital X auf einen starken Anstieg sogenannter DDoS-Angriffe: „In dieser Woche waren es bereits 23.000 DDoS-Angriffe, die wir im Netz sehen. Es geht exponentiell nach oben."

Marie-Agnes Strack-Zimmermann ordnete die Cyberbedrohung in einen größeren geopolitischen Zusammenhang ein. Neben Cyberattacken gehörten Desinformation und Angriffe auf Infrastruktur zu den Mitteln hybrider Auseinandersetzungen. „Und wir stehen unter Feuer, wir werden angegriffen", sagte die Vorsitzende des Ausschusses für Sicherheit und Verteidigung im Europäischen Parlament. Cybersecurity-Experte Thomas Köhler warnte zugleich davor, das Thema weiterhin als reine Technikfrage zu behandeln. Unternehmen könnten durch Cyberangriffe in ihrer Existenz bedroht werden; deshalb gehöre das Risiko in die Verantwortung der Unternehmensführung.

Auch für die operative Absicherung verschiebt sich damit der Maßstab. „Resilienz beginnt eben genau dort, wo der Normalbetrieb, die Idealbedingungen aufhören", sagte T-Systems-Vertriebsgeschäftsführerin Elke Anderl.

Für Unternehmen bedeutet das zugleich, Cyberabwehr nicht allein mit dem Kauf zusätzlicher Software gleichzusetzen. Telekom-Sicherheitsexperte Philipp Trinius sagte, entscheidend sei, das Security-Thema nicht „der IT-Abteilung irgendwo da unten im Keller" zu überlassen, sondern

zur Chefsache zu machen. Zusätzlich brauche es Menschen, die Informationen rund um die Uhr auswerteten und im Ernstfall reagierten: Es bringe nichts, lauter Systeme zu haben, aber nicht zu wissen „wie ich sie ausrolle und oder wer dann halt wirklich draufguckt und reagiert in dem Moment, wenn was passiert."

Genau hier liegt für den Mittelstand die Lücke. Drei Vollzeitkräfte beträgt der Median der Security-Teams von Unternehmen laut einer PwC-Befragung; 78 Prozent der Mittelständler beziehen bereits Managed Security Services. Die Frage verschiebt sich damit von „Welche Software haben wir?" zu „Wer erkennt und reagiert, wenn tatsächlich etwas passiert?" Hier will die Telekom Unternehmen u.a. mit „Security as a Service" unterstützen.

> *„Wir wollen Cybersicherheit demokratisieren – professionellen Schutz auch für kleinere Unternehmen verfügbar machen."*
>
> **Thomas Tschersich, Chief Security Officer Deutsche Telekom**

02 I Stimmen von der Digital X

„Bei aller Begeisterung über KI hilft es, die eigene Intelligenz zu bemühen. Deswegen ist es wichtig, Cybersicherheit ernst zu nehmen. Denn auch auf dieser Ebene wird versucht, unsere Gesellschaft auseinanderzutreiben.“

Dr. Marie-Agnes Strack-Zimmermann, MdEP

„Ab und zu passiert es, wie bei früheren Technologieentwicklungen, dass man seinen Verstand an der Kasse abgibt. Das ist ein Problem bei der Cybersicherheit. Die menschliche Firewall muss besser funktionieren.“

Prof. Thomas R. Köhler, Cybersecurity-Experte

„Sicherheit schützt die Normalität. Resilienz beginnt dort, wo in der Technologie der Normalbetrieb und die Idealbedingungen aufhören.“

Elke Anderl, Chief Commercial Officer T-Sytems

03 I Medieninformationen und aktuelle Nachrichten

Globale Unternehmensnetze: Vielfalt macht resilient
Cloud, KI und globale Geschäfte verlangen flexiblere Netze. T Secure Fabric verbindet deshalb Telekom-Infrastruktur mit Netzen und Technologien verschiedener Partner zu einer zentral gesteuerten Plattform. Unternehmen können neue Standorte, Clouds und Anwendungen schneller anbinden und bestehende Netze schrittweise modernisieren. Unterschiedliche Verbindungswege reduzieren zugleich die Abhängigkeit von einzelnen Providern und erhöhen die Ausfallsicherheit.
Mehr zu diesem Thema in der Medieninformation

Cyberangriffe stoppen, bevor das Geschäft stillsteht
Cyberangriffe werden für Unternehmen vor allem dann teuer, wenn Kasse, Telefonie oder Warenwirtschaft ausfallen. Die Telekom verlagert deshalb einen Teil der Abwehr direkt ins Netz: Verdächtige Verbindungen können erkannt und blockiert werden, bevor sie die Systeme der Kunden erreichen. Allein Security OnNet blockiert so monatlich mehr als 48 Millionen Bedrohungen. Ergänzende Managed Services bieten je nach Bedarf Ausfallsicherheit und 24/7-Cyberabwehr.
Mehr zu diesem Thema finden Sie hier

Blaulicht-Kommunikation bekommt Vorfahrt im 5G-Netz
Cyberangriffe Mit T Mission bringt die Telekom einsatzkritische Kommunikation ins 5G-Zeitalter. Sprache, Live-Videos, Lagebilder oder Sensordaten können direkt an die Einsatzkräfte gesendet werden -sicher und priorisiert, auch bei hoher Netzauslastung. Gleichzeitig verbindet T Mission die neue die MCx-Kommunikation mit dem bewährten Tetra-Funk. So können Einsatzkräfte mit Tetra- und MCx-Ausrüstung weiterhin miteinander sprechen. Wie das funktioniert, zeigt unser T Mission-Truck auf der Digital X.
Mehr zu diesem Thema finden Sie hier

Telekom macht Drohnen sichtbar
Die Telekom zeigt auf der Digital X erstmals live ihren Drohnen-Schutzschirm. Sensoren erkennen die Funksignale zwischen Drohne und Fernsteuerung und können so Drohne und Standort des Piloten lokalisieren. Die Daten werden an eine zentrale Leitstelle übertragen, damit Sicherheitskräfte die Lage schnell bewerten und reagieren können. Das System soll Flughäfen, Industrieanlagen und andere kritische Infrastruktur schützen.
Mehr zu diesem Thema in der Medieninformation

04 I Zahlen, Daten, Fakten

Cyber-Erpressung trifft vor allem den Mittelstand
Der deutsche Mittelstand steht besonders im Fokus von Cyberkriminellen: 90 Prozent der Opfer digitaler Erpressung sind laut BKA kleine und mittlere Unternehmen. Gleichzeitig zeigt eine PwC-Studie, dass viele Mittelständler ihre eigene Cyber-Abwehr überschätzen. Reifegradanalysen bewerten das tatsächliche Schutzniveau häufig ein bis zwei Stufen niedriger als die Unternehmen selbst.
Quelle: PwC, Cyberresilienz im Mittelstand 2026 / Originalquelle

90 %
der Opfer digitaler Erpressung sind KMUs

Ransomware steckt hinter fast jedem zweiten Datenleck
Es zeigt sich in 2026 eine weiter verschärfte Bedrohungslage: 48 Prozent aller untersuchten Datenlecks stehen inzwischen mit Ransomware in Verbindung. Gleichzeitig werden Software-Schwachstellen immer häufiger zum Einfallstor für Angreifer. Besonders kleinere Unternehmen sind überproportional von Ransomware betroffen und verfügen häufig über weniger Ressourcen zur Abwehr. Verizon analysierte für den Report mehr als 22.000 bestätigte Datenlecks in 145 Ländern.
Quelle: Verizon Data Breach Investigations Report 2026 / Originalquelle

48 %
Fast jedes zweite Datenleck hat inzwischen einen Ransomware-Bezug.

KI „verbessert“ Angriffsschutz
40-60.000 Anomalien bewerten lernende Systeme der Telekom jede Minute. KI hilft den Experten, den Durchblick und damit die Lage im Griff zu behalten.
Live-Quelle: www.sicherheitstacho.eu

40-60.000 Anomalien
im Check pro Minute

05 I Hintergrund: Wenn aus IT-Sicherheit Betriebsfähigkeit wird

Ein Alarm am Freitagabend zeigt, worum es bei Cybersecurity im Mittelstand zunehmend geht. Technik kann einen Angriff erkennen. Entscheidend ist aber, wer bewertet, entscheidet und reagiert, wenn das eigene IT-Team nicht rund um die Uhr besetzt ist.

Freitagabend, 18.30 Uhr. Auf einem Rechner in der Produktion eines mittelständischen Maschinenbauers wird verdächtiges Verhalten erkannt. Vielleicht ein Fehlalarm. Vielleicht beginnt gerade eine Ransomware-Attacke. Der IT-Leiter muss nun nicht nur wissen, welche Sicherheitssoftware installiert ist. Er muss klären: Ist das System kompromittiert? Hat sich der Angreifer bereits weiterbewegt? Muss der Rechner isoliert werden? Und wer trifft diese Entscheidung, wenn das kleine IT-Team längst im Wochenende ist?

Die Szene ist beispielhaft, aber das strukturelle Problem ist real. Professionelle Cyberabwehr ist eine permanente Betriebsaufgabe. Viele Mittelständler können die dafür nötigen Spezialisten nicht in eigener Schichtorganisation vorhalten. In der aktuellen PwC-Befragung unter 400 deutschen Unternehmen liegt der Median der Informationssicherheits-Teams bei drei Vollzeitkräften. 78 Prozent beziehen bereits Managed Security Services.

Von der Schutzsoftware zur Reaktionsfähigkeit

Damit verschiebt sich die Security-Frage. Über Jahre stand der technische Schutz im Mittelpunkt: Firewall, Virenscanner, Endpoint Security, Backup. Diese Komponenten bleiben nötig. Doch ein Alarm hat erst dann Wert, wenn jemand ihn einordnet und bei einem echten Angriff schnell genug handelt. Cyber Protect verbindet deshalb technische Erkennung mit Analysten und definierten Reaktionsprozessen. Ein Unternehmen muss kein eigenes rund um die Uhr besetztes Security Operations Center aufbauen. Es muss aber festlegen, welche Aktionen ein Dienstleister auslösen darf und wann die eigene Organisation entscheidet.

CyberProtect zielt auf genau diese Lücke

CyberProtect adressiert vor allem kleinere und mittelständische Unternehmen. Sicherheitsplattformen von Microsoft beziehungsweise CrowdStrike überwachen Endgeräte auf verdächtige Aktivitäten. Telekom-Spezialisten bewerten die relevanten Alarme rund um die Uhr und können Gegenmaßnahmen einleiten, bis hin zur Isolation betroffener Systeme.

KI verändert vor allem Tempo und Skalierung

Parallel verändert künstliche Intelligenz die Angriffsseite. Der Verizon DBIR 2026 nennt 15 Techniken, die durch generative KI zusätzlich begünstigt werden können. Dazu gehören Aufgaben, die sich automatisieren oder beschleunigen lassen: öffentliche Informationen auswerten, personalisierte Phishing-Texte erzeugen, Code analysieren oder Teile einer Angriffskette vorbereiten. Das bedeutet nicht, dass Cyberangriffe plötzlich vollständig autonom werden. Viele erfolgreiche Attacken beruhen weiterhin auf bekannten Schwachstellen wie gestohlenen Zugangsdaten oder menschlicher Täuschung. Neu ist vor allem die Ökonomie: Recherche und Variantenbildung werden billiger und schneller. Dadurch können Angreifer mehr Ziele mit besser angepasster Ansprache bearbeiten. Anders gesagt: Mit KI kann die „bekannte" Phishing-Mail eben echter wirken als heute.

Die eigene KI schafft neue Zugriffsrechte

Für Unternehmen kommt eine zweite Entwicklung hinzu: Sie setzen selbst mehr KI ein. Ein Agent kann E-Mails lesen, CRM- oder ERP-Daten abrufen, Dateien verändern oder Workflows starten. Damit wird er aus Security-Sicht zu einer neuen Identität mit Rechten. Je mehr ein Agent tun darf, desto größer ist der mögliche Schaden eines kompromittierten Accounts oder einer manipulierten Eingabe. KI-Sicherheit ist deshalb nicht nur Modellkontrolle. Sie hängt an klassischen Themen wie Identitätsmanagement, Berechtigungen, Protokollierung, Netzsegmentierung und menschlichen Freigaben. Die nächste Generation von KI-Anwendungen macht alte Security-Grundlagen nicht obsolet, sondern wichtiger.

Von Cybercrime zu hybriden Bedrohungen

Hinzu kommt der geopolitische Kontext. Der Rat der Europäischen Union sanktionierte am 13. Juli neun Personen und vier Organisationen im Zusammenhang mit russischen Cyberangriffen und Destabilisierungsaktivitäten. Die EU beschreibt ein Umfeld, in dem staatliche Strukturen, Cyberkriminelle, Hacktivisten und private Akteure teilweise dieselben Infrastrukturen oder Werkzeuge nutzen. Nicht jeder Ransomware-Angriff auf einen Mittelständler ist deshalb staatlich gesteuert. Für die Verteidigung ist die Unterscheidung im ersten Moment oft zweitrangig. Ein Unternehmen muss seine Produktion, Kommunikation oder Lieferfähigkeit unabhängig von der Motivation des Angreifers schützen und wiederherstellen können.

Security muss in Schichten funktionieren

Ein sinnvoller Schutz setzt deshalb an mehreren Stellen gleichzeitig an. Security OnNet blockiert beispielsweise bekannte schädliche Ziele bereits im Telekom-Netz. Starke Authentifizierung schützt Identitäten. Endpoint Security überwacht Geräte. Segmentierung begrenzt Bewegungen im Netz. Ein SOC erkennt und bewertet verdächtige Aktivitäten. Backups und Wiederanlaufpläne sorgen dafür, dass ein erfolgreicher Angriff nicht automatisch zum langen Produktionsstillstand wird.

Die Make-or-Buy-Frage wird strategisch

Für den Mittelstand ist das am Ende keine Kapitulation vor Komplexität, sondern eine Beschaffungsentscheidung. Ein Unternehmen muss nicht jede Fähigkeit selbst besitzen. Es sollte aber verstehen, welche Fähigkeit es einkauft, wie sie in den eigenen Betrieb eingreift und wo die Verantwortung bleibt.

Der relevante Sicherheitsmaßstab ist deshalb nicht die Zahl installierter Tools. Er zeigt sich am Freitagabend um 18.30 Uhr: Wer sieht den Angriff, wer darf handeln, wie schnell wird der Schaden begrenzt und wann läuft der Betrieb wieder?

06 I Ansprechpartner und Interviewangebote

Thomas Tschersich
CEO, Telekom Security

Kann sprechen über: aktuelle Bedrohungslage, Security Operations, Managed Security, KI in Angriff und Abwehr, Resilienz. **Welche Security-Fähigkeit darf ein mittelständisches Unternehmen niemals vollständig auslagern?**

Dr. Niklas Horstmann
COO Deutsche Telekom Security GmbH

Kann sprechen über: Secure Networking, Managed Networks, Betriebssicherheit und Souveränität. **Wie viel administrativen Zugriff muss ein Managed-Service-Anbieter bekommen, damit er schnell reagieren kann, und wie kontrolliert der Kunde diesen Zugriff?**

Kontakt via Corporate Communications, Christian Fischer
Tel.: 0228 181 – 49494
E-Mail: christian.fischer03@telekom.de oder medien@telekom.de